WebARX

Report

Website Security In 2020

The Biggest Problems And Challenges Explained

webarxsecurity.com

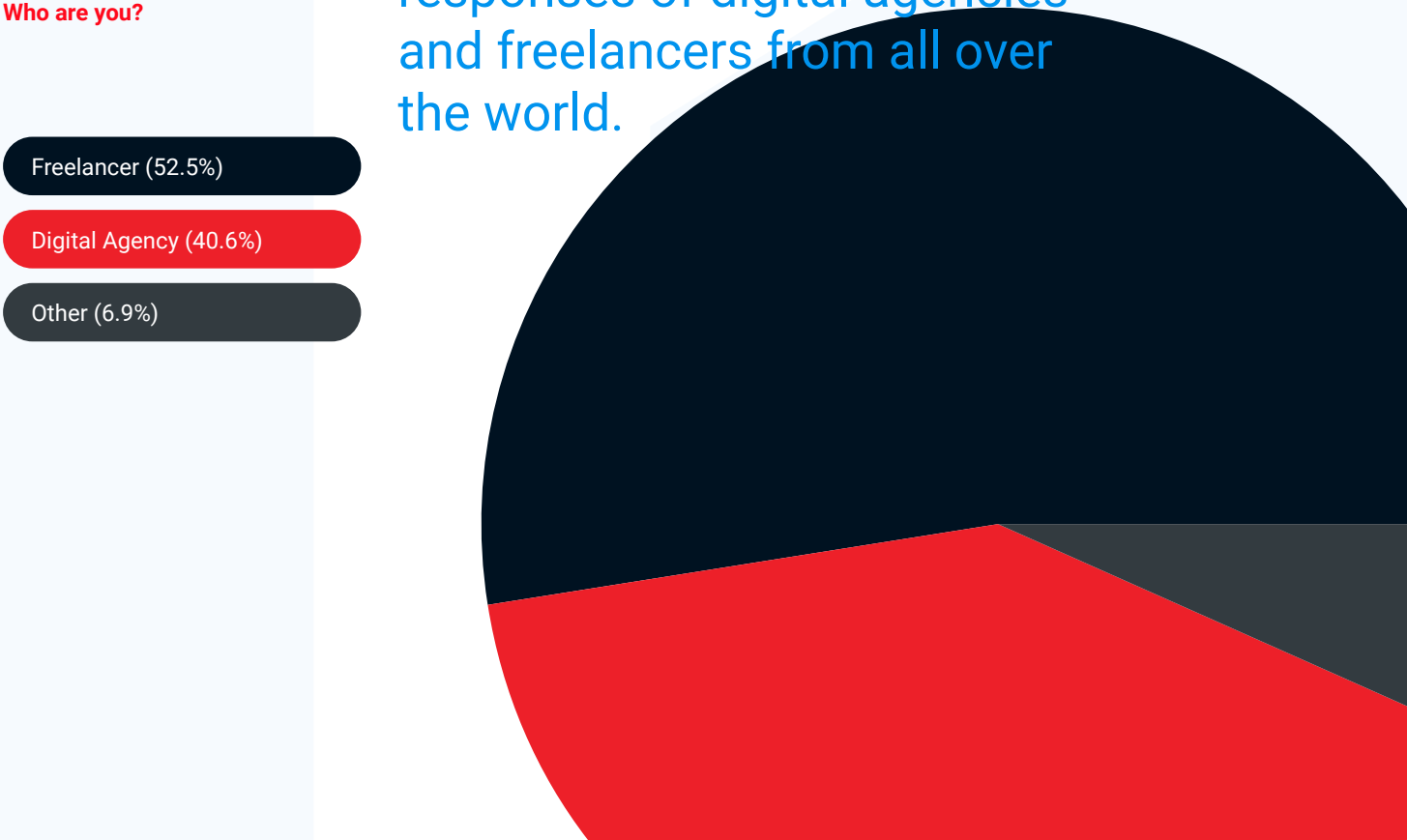
Over the past months, as the world has been shaken by the pandemic, cyber-attacks have increased and website security has become a major problem for many. Wide range of attacks have been targeting businesses, health organizations, and governments. Attacks were launched to spread malware, host phishing pages, steal credit card details, and more.

We wanted to know if web professionals who build and manage websites have witnessed the increased amount of malicious traffic and if it has affected their businesses in any ways.

We ran a survey to understand if the global crisis and an increased amount of cyber threats affect web professionals and website security as a whole. This website security report includes analysis from 338 responses of digital agencies and freelancers from all over the world.

This website security report includes analysis from 338 responses of digital agencies and freelancers from all over the world.

Who are you?



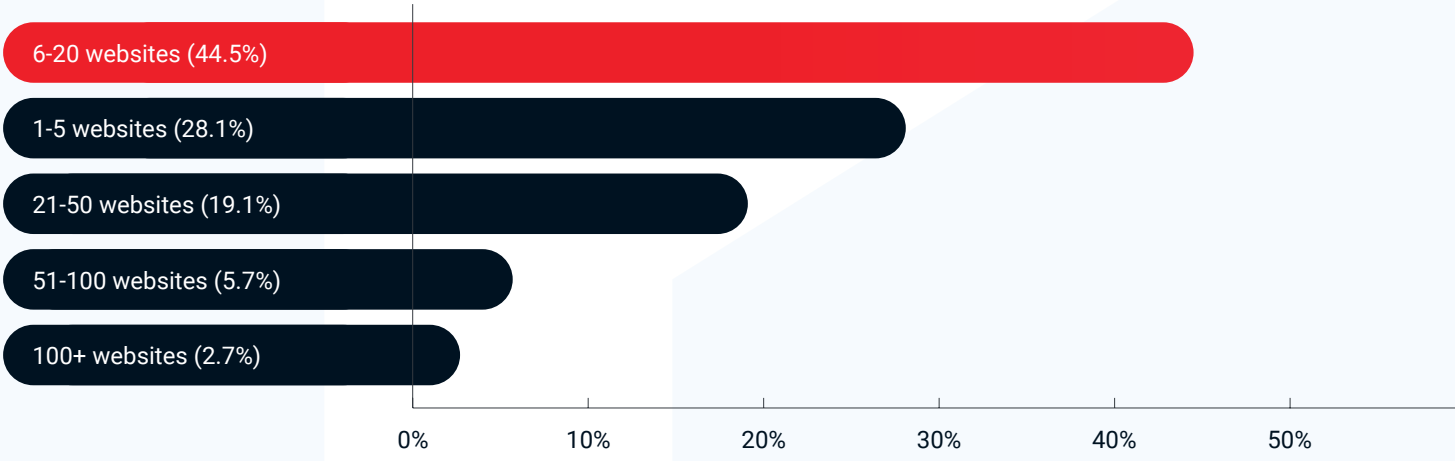
The responses to the website security survey were collected from several mastermind groups of digital agency owners and web developers. Little less than half of the respondents were incorporated digital agencies.

Over half of the respondents were freelance web professionals. The remaining 6% of the respondents were website owners, business owners, bloggers, and non-governmental organizations.

About 80% of freelancers that participated in our website security survey stated that they are responsible for less than 20 sites. On the other hand 44% of digital agencies that participated stated that they are responsible for over 20 sites.

Most of the respondents (72%) have more than 6 websites in their portfolio.

How many websites are you responsible for?



About 8% of respondents have 50-100+ sites and 90% of them are digital agencies.

Agencies don't just have more demanding customers, they also have more challenges to maintain and secure a larger amount of websites the customers keep them responsible for.

WordPress continues to dominate

Agencies and freelancers who participated in the survey use a variety of content management systems and coding languages to build websites for their customers.

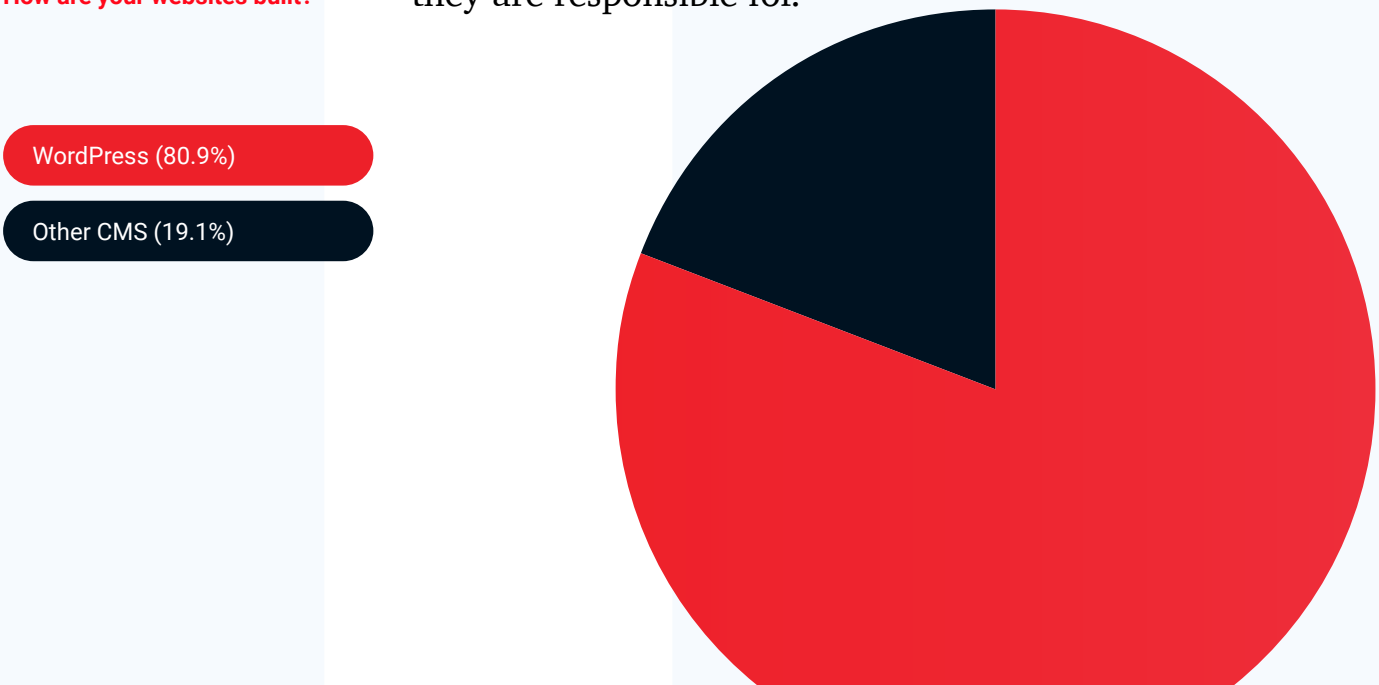
The most popular CMS among 80% of the respondents is WordPress.

The top content management systems mentioned were **WordPress**, **Magento**, **Drupal**, and **Joomla**. Top programming languages included PHP and Javascript with the use of frameworks such as Laravel, Node. Js, and React.Js. A small minority has also made use of managed services and website builders such as Squarespace, Webflow, and Wix.

Web professionals are increasingly worried about website security

243 (ca 74%) respondents in the survey stated that they are increasingly worried about website security. The data revealed that only a little less than half of them (45%) take proper measures to protect the sites they are responsible for.

How are your websites built?

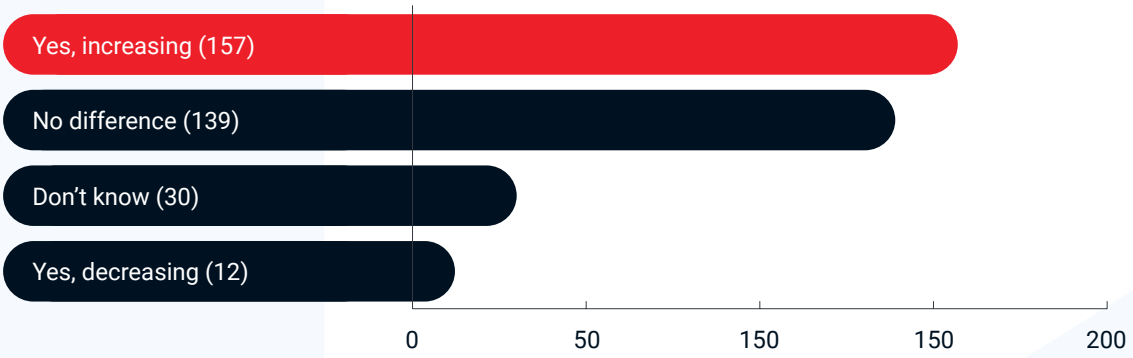


Website attacks are increasing

Close to 43% of the respondents have seen an increase in attacks targeted to the websites they are responsible for. Surprisingly there were 30 respondents who have no insights if the attacks have increased or not.

When attacks are detected, it does not mean they were successful. We at **WebARX** see millions of attacks targeted to the websites we protect. These attacks are blocked, logged, and monitored in real-time to make sure the malicious traffic will be rejected.

Have you seen a change in the amount of attacks targeted against your websites?



One reason for the increased attacks could be linked to a large number of vulnerabilities disclosed in popular WordPress third-party code such as plugins, themes, and other dependencies.

For example, in the first 5 months of 2020, we have seen over 200 vulnerabilities that have affected more than 40 million websites.

We also discovered that **25% of the responders have seen a hacked website in the past month** prior to participating in the survey. This gives us an understanding of the magnitude of the problem.

Websites are infected with malware and used to run further attacks against other websites and businesses. Hacked websites are often used to direct traffic to malicious sites, to steal credit card information and in some cases to even infect the visitor's computers.

Additionally, hosting phishing pages on hacked websites has become an increasingly popular tactic to steal credentials of third-party services.

Meanwhile, E-commerce websites are often targeted to inject websites with javascript based keyloggers to steal credit card details of online shoppers.

While gaining access to one small website might not be too valuable, exploiting a popular plugin can give the attacker access to hundreds of thousands or even to millions of sites with a single coordinated attack.

Web professionals are becoming more security-aware

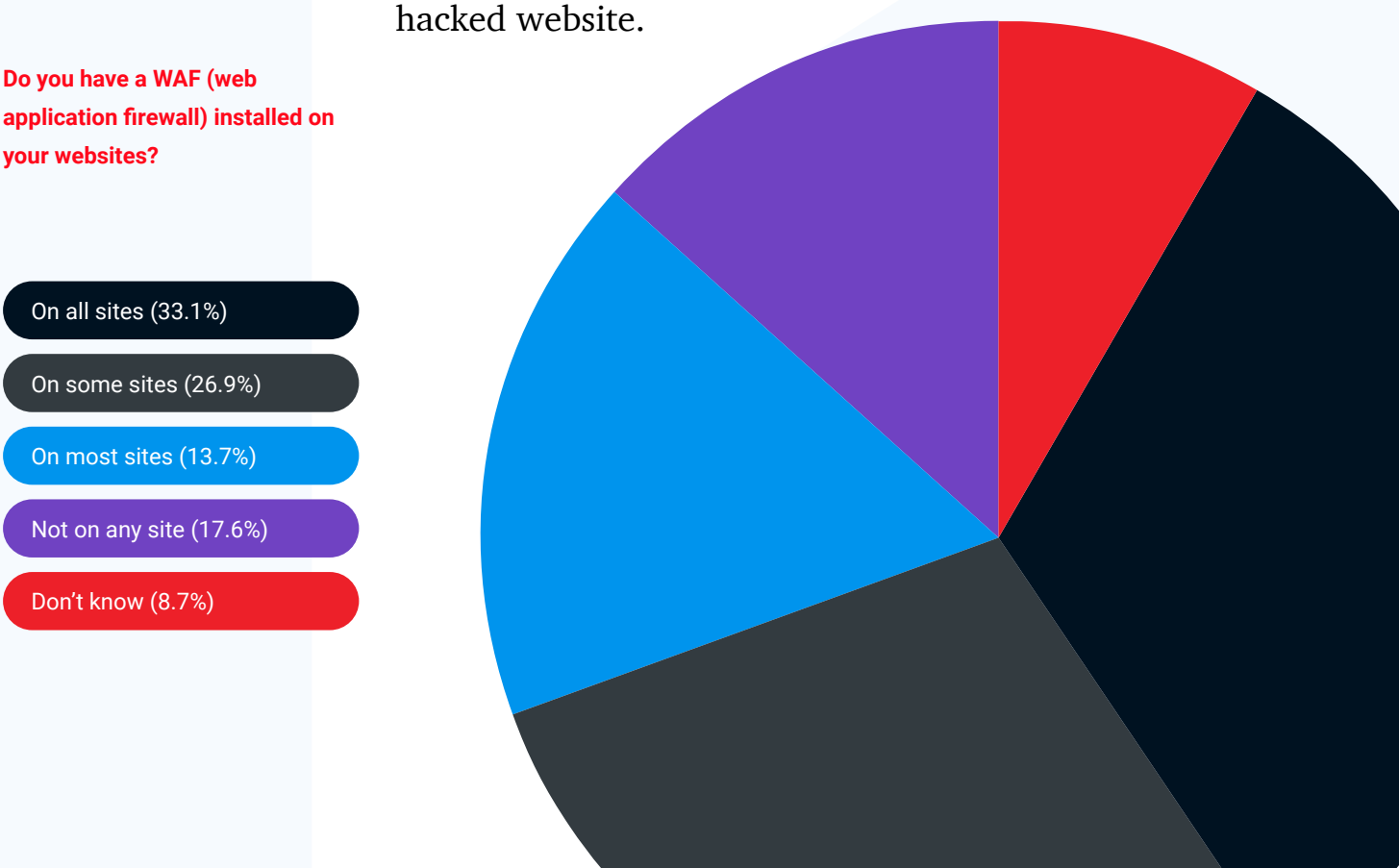
We asked from the participants of this survey if they have a web application firewall protecting their sites and the results showed that **over half of the freelancers (53%) and agencies (57%) have a firewall installed** on most or all of the sites they manage.

About 17% of the participants don't protect any of their websites with a firewall and **8% have no overview** of the security of their site and do not know if they have a firewall installed or not.

At the same time, almost one-third of the participants (29%) who don't use a firewall to protect their sites but are concerned about their website security have witnessed hacked sites in the past months.

The data shows a direct correlation between the unprotected websites that are not protected by a web application firewall and a chance of witnessing a hacked website.

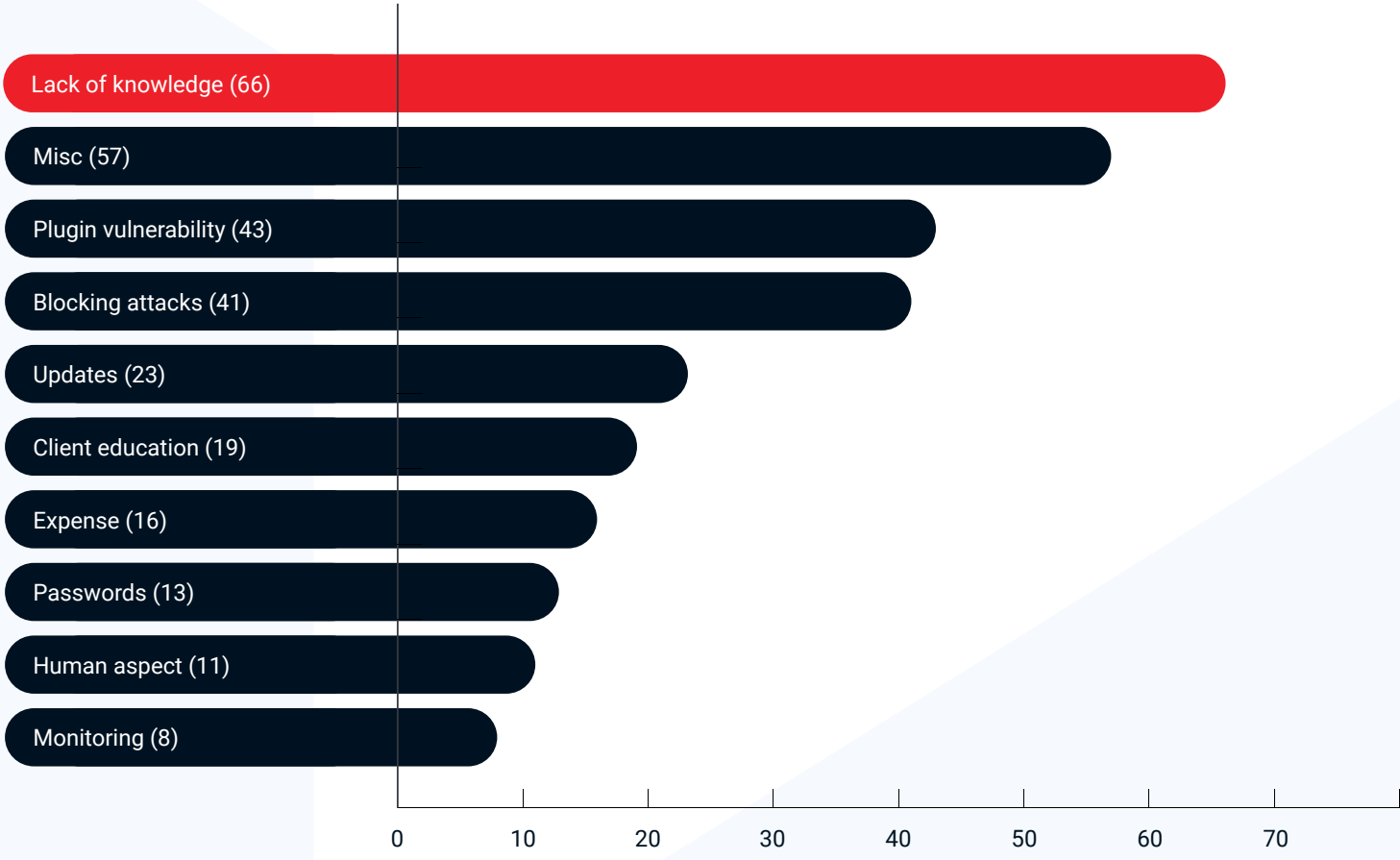
Do you have a WAF (web application firewall) installed on your websites?



What challenges are web professionals facing?

We asked the participants of the survey to explain their challenges in detail which **gave insights into more than five hundred different challenges** which we sorted into 10 main categories.

In your experience, what is the biggest challenge in securing websites?



The biggest category of challenges was the lack of knowledge. Second was a selection of different tasks and problems that freelancers and agencies have problems with, which did not fit any of the remaining 9 categories. Others consisted of attack prevention, plugin vulnerabilities, client education, and more.

Lack of website security knowledge

Respondents mentioned the lack of knowledge on how to secure a site and how to keep it protected. They struggle with the complexity of security tools and the installation process can be taunting. Additionally, many find it hard to understand if a given security solution really works or not. Additionally, we also saw that it's hard to understand if a given security solution/product really works or not.

Many freelancers mentioned that they don't know the steps required to secure the websites and digital agencies, on the other hand, highlighted the complexity of finding the right tool for the job.

Tips

- Always think about security as an ongoing process, not something you can just install and forget.
- High quality and responsive customer support often overweighs technical advancement of the product.
- Look at what the security companies do, not what their marketing claims. Their own security research is a good thing to start with.

How to find a security tool that fits your needs?

There are many options available on the market. When looking at all the existing solutions, one could divide these tools into three categories:

reactive
proactive
and a combination of both

The reactive security tool is something that helps you deal with the consequences of an attack. A good example is a **malware scanner**. A malware scanner in its essence is to locate already injected malicious code on the site.

The proactive security tool is something that helps you prevent the attacks. A good example is a **vulnerability scanner** and a web **application firewall**. It allows you to address the potential security issues to avoid malware infections and breaches in the first place.

A good approach is to add layers to your website security

The first layer would be the security awareness itself, keep yourself up to date with the information regarding the latest threats, and make sure you have a proper overview of what is happening on your website. Also take time to carefully choose reliable and trusted service providers for your cloud hosting requirements and for the development stack you use (plugins/ themes, etc.).

The second layer would be your first line of defense. Modern attacks are largely automated, so it's important for you to automate protection as well. Set up a vulnerability monitoring solution and a managed web application firewall that can provide necessary protection against threats such as 0-day and 1-day vulnerabilities.

Use code websec2020 to try WebARX for vulnerability monitoring and managed web application firewall for free (2 months)!

Your third layer should include proper logging, malware scanner, and a reliable backup solution. If one of the first two layers fail, your third layer of defense should be able to detect anomalies and allow you to act fast and efficiently.

Tips

- Keep up with threats: wpvulndb, Hackbusters, NVD
- Pevent attacks: ModSec, Cloudflare, WebARX
- Remediation: AI-Bolit, Sitecheck, URLscan

Blocking and preventing attacks

Over 40 respondents of the website security survey stated that their main challenge is blocking and preventing attacks targeted to their websites. See a few examples of mentioned challenges below:

"Automated protection, reports. Ability to have an overarching dashboard for a single site as well as a view for all sites."

"Prevent attacks with a proven firewall."

"Blocking the bots out by not affecting good bots and the users."

"Constantly checking new vulnerabilities and blocking attacks on all sites."

Invest into managed WAF to block attacks

There are two main types of firewalls on the market: a cloud-based WAFs and an endpoint WAFs.

Cloud WAF for reducing bot traffic and preventing DDoS attacks

A cloud-based web application firewall is like a middle-man between your site and the visitor. When a visitor enters your domain name to the browser, the connection goes to the cloud-based firewall provider servers, where it's analyzed. If the visitor does not pose any risk to the site, the traffic is forwarded to the actual website (or to the cached version of the site).

Endpoint WAF is for protecting the website from more sophisticated and direct hacking attempts

Endpoint web application firewall (endpoint WAF) runs within the application or in the server itself. It's often aware of the environment such as the software used inside the website and understands how it's built. Endpoint WAF has an internal overview of how the software is behaving and understands who are the visitors by their permissions and if they are authenticated or not. Just like a cloud-based WAF, it blocks attacks and filters unwanted traffic.

What does managed WAF mean? New threats are discovered on a daily basis. Threat intelligence is a critical element that differentiates very good WAF solutions from the average. A large amount of data is often used to teach machine learning algorithms and managed web application firewall providers invest heavily in vulnerability research to feed your firewall with the latest information about the emerging threats. Thus they manage and update the firewall rules for you.

Which firewall to choose? The truth is, you should use both.

Good overview of the pros, cons, and differences of endpoint and cloud WAF can be seen here.

Plugin vulnerabilities are posing the biggest risk

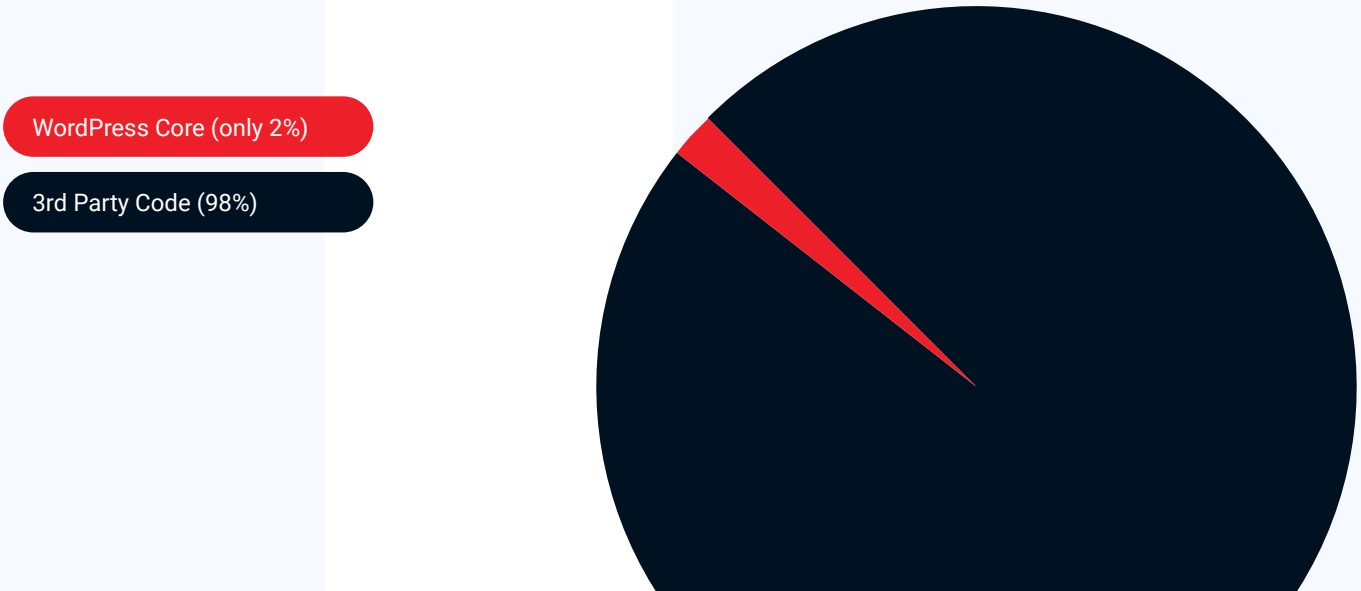
A significant amount of participants mentioned that their biggest challenge is plugin vulnerabilities or zero-day vulnerabilities in third-party code. This is a problem, we at WebARX are focused to provide solutions for. WordPress is a very good example of the magnitude of that issue.

A very worrisome fact about website security statistics: 98% of WordPress vulnerabilities are related to plugins.

Anyone can create a new plugin and add it to the WordPress repository. While this is very convenient, it raises many concerns, since the skills of the plugin developers vary. For the majority of the WordPress users, it's hard to tell which of the plugins are written poorly and which ones are not.

If you have the necessary skills then you could audit the code, but vulnerabilities can also be introduced with plugin updates which many struggle updating, let alone audit each and every change.

WordPress third-party vendor vulnerabilities in 2018. (Source: WP White Security)



Importance of vulnerability monitoring in website security

First things first. Do you even have an overview of how Many people don't even have an overview on all the dependencies such as plugins, themes, and third-party code their website relies on. Before one can benefit from vulnerability monitoring, it would help to know what to monitor.

Security solutions such as WebARX will detect all the different plugins within the website and will then analyze if any pose a threat to the websites security. Receiving such information automatically and as quickly as possible is critical for being able to address issues in time.

We have in many cases witnessed large-scale attacks against vulnerabilities the same day the developer released a fix. It's a matter of days if not hours to address the vulnerabilities and doing so manually (especially with many sites and dependencies) can be an extremely difficult task.

Tips

- Try to use as few dependencies (plugins/themes) as possible.
- Monitor the security of your dependencies (wpvulndb, WebARX, Snyk).
- Use a managed web application firewall that provides virtual patches to the software you use (Sucuri, WordFence, WebARX).

Keeping up with all the software updates

Updates are a problem many digital agencies and freelancers have trouble with. In this survey, we had 22 respondents that said it is one of their main challenges.

There were two main problems that web professionals are facing. The most popular was about third party plugin updates and how to keep them protected. The second main problem was how to keep everything up to date without breaking the site.

Many plugins receive regular updates. These updates often include new features, bug fixes, or security fixes which are important to keep your sites safe. When it comes to security updates, you should always update the software whenever such updates are available.

When we talk about other updates like new features or core updates, it is advised to wait a few days because some major updates might break your site. You can keep an eye on forums and see if anyone else has any issues with the latest update. This allows you to make sure the update will be beneficial.

Updates still, even with forum monitoring and research, need to go hand-in-hand with backups. If you have regular backups and perform a backup before updating your site, you can restore your site from a backup if the site still breaks.

Tips

- Automate the CMS updates: MainWP, Watchful
- Keep number of dependencies low. If possible, enable automatic updates.
- Keep frequent backups, off-site.

Educating clients about website security

A big part of the respondents stated that their main challenge is to educate their clients about security. The challenges were not only about if website security is needed, but also the dangers of installing nulled plugins, old and outdated plugins, and more.

Majority of clients don't understand why their small website is targeted by hackers and therefore they can't understand the importance of securing their websites. The hard conversation about explaining extra cost for security was also mentioned several times.

Another issue with client education was about malware removal and hacked sites. Freelancers and agencies have problems explaining why the site is hacked, who would do that, and why the developer is not responsible. In addition to that, how to tell the angry client that a service like malware removal is for an extra cost.

Without the up-front discussion about potential risks of having a website – the reputation of an agency or a freelancer can later suffer.

Increase trustworthiness and add value

One of the best things you can do is educate your clients. It builds trust. When your client has several options to choose from, he or she will most definitely choose the option that has educated them the most.

So first thing when either selling care plans or up-selling security to your client is to prepare some content (or use content previously prepared by a security company), videos, or documents to address the most frequent questions, such as “why would anyone want to hack my small website?”.

The smart consumer will opt to buy from the company that’s educated him on the issue and presented him with multiple solutions. That company’s selflessness has built trust — and its ability to teach him has bought his loyalty in the future.

– Mark Quinn

Tips

- Talk about security as early as possible. This can be seen as additional value and shows responsibility.
- Add security as a dedicated section to the handbook which you provide to your customer.
- Include security awareness within a newsletter. Find monthly summaries from our security blog.

Explaining costs of website security solutions

It should never be a goal by itself to find the cheapest option. If the website is important enough to have been built in the first place, it is generating revenue, representing a business or collecting important data – the cost of security is usually a fraction of what you would lose after a security incident.

The heavy research and development these companies do for building an outstanding product, and to keep your websites security one step ahead from hackers requires significant investment. The cost of a security service often reflects also on the quality of support and on the responsibility the company takes.

Once you have a list of potential solutions, take a look at the reviews about their support and product. Since security is very research-intensive, don't forget to look if the company is doing their own security research to stay ahead from malicious actors.

Tips

- Show the data. The probability of a breach is high and the cost of remediation is always higher than prevention.
- Additional responsibility is often taken by the security company to provide rapid reaction. Read more about it.
- Introduce customers to multiple comparable solutions.

Importance of passwords and access management

It's no surprise that people use bad passwords. Passwords are hard to remember. When it comes to security, experts advise using unique passwords for each account online, which does not make remembering passwords any bit easier.

The top 5 most frequently used passwords (source):

123456, **123456789**, **qwerty**, **password** & **111111**

Hopefully, your password is not on that list. A good way to have strong passwords is by using a password management tool. With a password management tool, you can start using complex randomly generated passwords to make sure they are unique.

Password management tools are good for several reasons:

Firstly – you won't remember every password you have and it's bad practice to use one password in more than one account.

Secondly – use pass**phrases** (short sentence) or generate a random key with your password management program.

Thirdly – you can easily access all your passwords from one place with one **master key**.

Tips

- Good options for a password management tools are: Lastpass, Keepass, 1Password.

Adding a second layer of protection

For second layer protection, you should add two-factor authentication (**2FA**), also called multiple-factor or multiple-step verification to your important accounts. Two-factor authentication is an authentication mechanism to double-check that your identity is legitimate.

It is something that will keep your accounts more secure and offers you an extra layer of protection, besides passwords. It's hard for cybercriminals to get the second authentication factor (which is often your smartphone) and it will drastically reduce their chances to succeed.

2FA is a must-have for:

Your work or personal email

Your cloud storage accounts (Google Drive, Dropbox)

Online banking

Social media accounts (Facebook, Twitter, LinkedIn)

Communication apps (Slack, Skype)

Online shopping (PayPal, Amazon)

Your password management apps

Website administrator accounts

Enable 2 factor authentication where you can. Both SMS and authenticator apps are good choice. You can see how to add 2FA to your website administrator accounts here.

Reducing human errors

People often make mistakes without realizing how the mistake can affect the organization or a company. Human mistakes were the cause of 21% of data breaches in 2018 according to the 2019 Data Breach Investigations Report made by Verizon.

Despite all the security tools, firewalls, checklists and tweaks you make to your website, there is always a possibility that your site ends up hacked because of a simple human mistake.

What are the common mistakes people do:

- Sending passwords or valuable data via email (in some cases to the wrong place).
- Being tricked into installing malware (for example nulled WordPress plugins/themes).
- Being tricked into submitting credentials to a fake login page, also called a phishing page.

Phishing and other types of scams are often executed very professionally and can sometimes trick even seasoned security professionals. Unfortunately, humans can't be patched and there is no firewall that can prevent well crafted social engineering attacks. What can be done is to regularly keep up to date with threats and educate people on cyber hygiene.

Here is an example of a scam targeted to scare website owners to pay ransom for their hacked website.

Tips

- A good source to keep up to date is Hackbusters.
- Keep in mind that if something looks too good to be true, it probably is.

Conclusion

The global crisis has accelerated the digitalization of society and businesses continue to move online. Digital agencies and web professionals who are in the front-line by providing web development and IT services are becoming increasingly worried about the security.

The number of attacks is growing and even the smallest websites are hit by automated hacking tools. While businesses move online and E-commerce is growing rapidly, criminals find new ways to make money by luring people into elaborate scams or straight away infect websites with various malware and to steal credit card details of online shoppers.

The biggest challenge for website security seems to be the heavy use of third-party code which also counts for the majority of security vulnerabilities in the most popular content management system, WordPress.

On the other hand, web professionals are becoming increasingly aware of security risks and more companies are providing help with security services, tools, and support.

Now, it's time to educate the end-users and customers and share this website security report with them.